# CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022

June 2022



## **CIRCIA Overview**

In March 2022, Congress enacted the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)

#### H. R. 2471-990

- (2) CONGRESSIONAL LEADERSHIP.—The term "congressional eadership" means—
  - (A) the majority leader of the Senate;
  - (B) the minority leader of the Senate;
  - (C) the Speaker of the House of Representatives; and (D) the minority leader of the House of Representa-
- (3) SERGEANTS AT ARMS.—The term "Sergeants at Arms" means the Sergeant at Arms and Doorkeeper of the Senate, the Sergeant at Arms of the House of Representatives, and the Chief Administrative Officer of the House of Representatives.

### DIVISION Y—CYBER INCIDENT REPORT-ING FOR CRITICAL INFRASTRUCTURE ACT OF 2022

#### SEC. 101. SHORT TITLE.

This division may be cited as the "Cyber Incident Reporting for Critical Infrastructure Act of 2022".

#### SEC. 102. DEFINITIONS.

#### In this division:

- (1) COVERED CYBER INCIDENT; COVERED ENTITY; CYBER INCIDENT; INFORMATION SYSTEM; RANSOM PAYMENT; RANSOMWARE ATTACK; SECURITY VULNERABILITY.—The terms "covered cyber incident", "covered entity", "cyber incident", "information system", "ransom payment", "ransomware attack", and "security vulnerability" have the meanings given those terms in section 2240 of the Homeland Security Act of 2002, as added by section 103 of this division.
- (2) Director.—The term "Director" means the Director of the Cybersecurity and Infrastructure Security Agency.

#### SEC. 103. CYBER INCIDENT REPORTING.

(a) CYBER INCIDENT REPORTING.—Title XXII of the Homeland

- Requires the Cybersecurity and Infrastructure Security
  Agency (CISA) to coordinate with Federal partners and
  others on various cyber incident reporting and ransomware
  related activities
- Requires CISA to establish a new regulatory program requiring reporting of certain cybersecurity related items



# **CIRCIA Key Elements**

**Cyber Incident Reporting Initiatives** 

### **Ransomware Initiatives**

Regulatory
Reporting Requirements

**Cyber Incident Reporting** 

Covered entities must report to CISA any covered cyber incidents within 72 hours after the entity reasonably should have believed the covered cyber incident occurred

### **Ransomware Payment Reporting**

Covered entities must report to CISA any ransomware payments within 24 hours of making the payment. CISA must share such reports with Federal agencies, similar to incident information

## Federal Incident Report Sharing

Any Federal entity receiving a report on a cyber incident after the effective date of the final rule must share that report with CISA within 24 hours. CISA will also have to make information received under CIRCIA available to certain federal agencies within 24 hours.

# Ransomware Vulnerability Warning Pilot Program

CISA must establish a pilot to identify systems with vulnerabilities to ransomware attacks and notify the owners of those systems

## **Cyber Incident Reporting Council**

DHS will establish and Chair an intergovernmental Cyber Incident Reporting Council to coordinate, deconflict, and harmonize Federal incident reporting requirements

### **Joint Ransomware Task Force**

CISA, in consultation with the National Cyber Director, Attorney General, and FBI, shall establish a task force to coordinate an ongoing nationwide campaign against ransomware attacks

Info Sharing and Coordination



# **CIRCIA Rulemaking Process**

Before CIRCIA covered cyber incident and ransomware payment reporting requirements go into effect, CISA must develop and issue regulations





- CIRCIA requires that CISA publish a Notice of Proposed Rulemaking (NPRM) within 24 months of enactment of the statute
- CIRCIA also requires CISA to publish Final Rule within 18 months after publication of NPRM

# Voluntary Sharing of Incident Information

CISA encourages organizations to continue voluntarily reporting cyber incidents while CIRCIA reporting requirements are developed.

- Organizations are not required to submit cyber incident or ransomware payment reports to CISA until the yet-to-be-determined effective date of the Final Rule.
- CISA encourages organizations to continue voluntarily sharing cyber event information with CISA throughout the rulemaking period prior to the effective date of the Final Rule.
  - When cyber incidents are reported quickly, CISA can use this information to render assistance and provide warning to prevent other organizations from falling victim to a similar attack. This information is also critical to identifying trends that can help efforts to protect the homeland.
- Organizations can report unusual cyber activity and/or cyber incidents to report@cisa.gov or (888) 282-0870.





# For more information: CISA.gov/CIRCIA

For questions: CIRCIA@cisa.dhs.gov